

Secure and efficient elliptic curve-based certificate-less authentication scheme for solar-based smart grids

Reduanul Bari Shovon¹, Ashif Mohammad², Rimi Das³, Tuhin Hossain¹, Md Ahasun Habib Ratul⁴,
Ronjon Kundu⁵, Md. Ahsan Arif¹

¹Department of Computer Science and Engineering, Faculty of Engineering and Technology, University of Scholars, Dhaka, Bangladesh

²Institute of Energy, Faculty of Engineering and Technology, University of Dhaka, Dhaka, Bangladesh

³Department of Electrical and Computer Engineering, College of Science and Engineering, Idaho State University, Idaho, United States

⁴Faculty of Advanced Computer Science and ICT, Abdul Kadir Molla International School, Narsingdi, Bangladesh

⁵School of Engineering, University of Western Australia, Perth, Australia

Article Info

Article history:

Received Jun 8, 2024

Revised Nov 22, 2024

Accepted Nov 28, 2024

Keywords:

Authentication

Certificate-less cryptography

Elliptic curve cryptography

Scyther

Solar-based smart grid

ABSTRACT

Solar-based smart grids have emerged as a transformative force, encapsulating a paradigm shift towards decentralized and sustainable power generation. However, this evolution is accompanied by growing concern-authentication challenges that pose a substantial threat to solar-based smart grids' security. Existing work done by researchers reveals a gap in addressing these authentication issues, resulting in vulnerabilities that compromise the overall security and performance of solar enabled smart grid infrastructures. In response to these concerns, this paper suggests a novel certificate-less authentication scheme designed explicitly for solar-based smart grids. Our technique, which uses elliptic curve (EC) encryption, mitigates authentication problems and navigates the resource limits inherent in a smart grid environment. The security evaluation also shows that our mechanism security is higher in terms of the security attributes it delivers. Supported by a Scyther-based protocol specification, our solution undergoes a rigorous security analysis, demonstrating its robustness and effectiveness in critical security attributes. Furthermore, a performance evaluation underscores the efficiency of our scheme, positioning it as a robust, and effective solution for fortifying solar-based smart grid environments against evolving cyber threats.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Ashif Mohammad

Institute of Energy, Faculty of Engineering and Technology, University of Dhaka

Dhaka, Bangladesh

Email: ashif028628@gmail.com

1. INTRODUCTION

The inception of the smart grid has been a transformative milestone in the evolution of the electrical industry, heralding a new era of efficiency, reliability, and sustainability. As a sophisticated electrical grid system that employs a vast network of automated controls and modern communication technologies, the intelligent grid ensures bidirectional communication between utility providers and consumers, providing up-to-the-minute data and the capability to react dynamically to changes in electricity demand and supply [1]. Building upon this foundational innovation, incorporating solar energy into the smart grid infrastructure has resulted in the solar-based smart grid further revolutionizing the sector [2].

A solar-based smart grid marries photovoltaic technology with advanced grid infrastructure to create a responsive and dynamic energy system. During peak sunlight hours, solar panels installed on homes, businesses, and dedicated solar farms convert sunlight into electricity, either used immediately or stored in

batteries for later use. Smart grid technology enables this energy to flow where needed, optimizing distribution based on real-time consumption data [3]. It also facilitates two-way communication between energy consumers and utility companies, allowing for automated energy management and immediate adaptation to changing energy patterns. As a result, solar-based smart grids provide a renewable energy source and enhance grid stability and energy efficiency through intelligent distribution and storage solutions [4].

These systems rely on interconnected digital controls and communication protocols to operate efficiently, creating multiple entry points for cyber-attacks. As smart grids become more integrated with internet of things (IoT) devices and other internet-dependent technologies, the risk of unauthorized access and control by hackers grows. Cyber adversaries can exploit these vulnerabilities to disrupt power distribution, access sensitive data, or even cause physical damage to the infrastructure [5].

The authentication mechanisms used to provide security often rely on public key infrastructure (PKI), where two primary cryptographic techniques are employed: identity-based cryptography [6] and certificate-based cryptography [7]. Identity-based cryptography can be less secure due to its reliance on a central authority for key generation, creating a single failure point. Certificate-based cryptography, while robust, suffers from complex certificate management and the risk of certification authority (CA) compromise. The solution lies in certificate-less cryptography [8], which eliminates the need for CAs, thereby reducing overhead and avoiding the pitfalls of centralized key generation.

Regarding cryptographic operations, authentication mechanisms heavily depend on Rivest-Shamir-Adleman (RSA) and bilinear pairing. Nonetheless, these mechanisms could be better for resource-limited environments like smart grids due to their reliance on larger key sizes and time-consuming operations. In such scenarios, elliptic curve cryptography (ECC) is preferred. It provides security with smaller 160-bit key sizes and requires less time for its operations [9].

Building upon the earlier discussion, this paper introduces a novel scheme known as the certificate-less authentication scheme for smart grid. This work presents several key contributions with rigorous security analysis and performance related assessments that represents its resilience against a range of cyber threats and its superiority over existing authentication mechanisms.

Considering the security and resource constraints within solar-based smart grids, we introduce a certificate-less authentication scheme based on an elliptic curve (EC) tailored for solar-based smart grid applications. We have also developed a high-level protocol specification language code for our scheme in Scyther, and the findings indicate the safety and security of our proposed solution against various security attacks. Our work undergoes a comprehensive security analysis, focusing on crucial security attributes such as authentication, integrity, non-repudiation, and resistance to known attacks. Compared with existing solutions, the outcomes we obtained distinctly establish the superiority of our approach to security effectiveness. Furthermore, we compare performance and evaluate computational cost and communication overhead. The outcomes reveal the efficiency of our scheme, rendering it well-suited for resource-limited solar-based smart grid environments.

2. PRELIMINARIES

2.1. Elliptic curve

In 1987, Neal Koblitz introduced the concept of EC [10], wherein an EC is termed an algebraic curve with a genus equal to 1. An EC over a field K (where a field is a mathematical framework enabling the operations of subtraction, multiplication, and division) is specified by an equation of the form [11]:

$$y^2 = x^3 + ax + b$$

in the above equation, $a, b \in K$ and the curve contain the set of solution $(x, y) \in K \times K$ that satisfies this equation, along with the additional point at infinity, which serves as the identity element with the group structure associated with the curve.

2.2. Elliptic curve discrete logarithm problem

EC discrete logarithm problem (ECDLP) is the fundamental problem underlying the security of ECC. It involves finding the value of j from [12]:

$$Q = j \cdot P$$

in the above equation, P and Q are points on the curve, and j is an integer. The problem is determining the value of j when you are only given points P and Q on the curve. The computational complexity of solving this problem underlies the security of many EC-based cryptographic schemes [12].

3. RELATED WORK

Authentication techniques are critical to the security of smart grid operations and regulate access and data reliability within complex energy networks. This section examines various modern authentication mechanisms, examining their significance, constraints, and flexibility within the complex domain of smart grid environments. Vallent *et al.* [13] efficiently built a novel anonymous authenticated key agreement system based on EC encryption. The plan satisfies the standard and extended Canetti–Krawczyk (eCK) security standards, as demonstrated by both formal and informal security analyses. But this work has the absence of results from actual empirical performance evaluations. Badshah *et al.* [14] addressed and devised a new scheme called the lightweight authenticated key exchange strategy for a blockchain-enabled smart grids environment (LAKE-BSG), which enables safe communication between service providers (SPs) and smart meters (SMs) using blockchain safeguard data network. Using a consensus mechanism, SPs are responsible for validating newly added blocks to the private blockchain. For the LAKE-BSG security purpose analyzation, this study used the real oracle model and formal security verification using the Scyther tool. The shortcoming of this scheme is the absence of detailed discussion on the scalability and computational overhead. In this paper, Shukla *et al.* [15] developed a blockchain-based system model for secure communication in addition to a unique advanced elliptic curve cryptography digital signature (AECCDS) algorithm using fog computing (FC). In this scenario, FC nodes will act as miners at the SMs edge to facilitate safe, instantaneous connection. This paper lacks insights the latency implications of the mining process and also not exploring the impact on performance and efficiency while scaling to manage a high number of SMs.

In their paper, Deng and Gao [16] introduced a certificate less authentication mechanism for smart grids. It sidesteps certificate and key escrow issues in prior schemes reliant on traditional cryptography. However, it lacks more effective robustness against replay and man in the middle attack. Khan *et al.* [17] designed a lightweight authentication and key agreement protocol for the evolving smart grid, addressing security, and privacy concerns. Through AVISPA verification, the protocol's correctness and robustness are validated, showcasing its superiority. Cui *et al.* [18] introduced a novel authenticated key agreement model based on certificate-less public key cryptography (CL-PKC) tailored for the power IoTs. The proposed scheme, validated under the eCK security model, emphasizes simplicity and efficiency in key agreement protocols for power IoT communication. Through simulations, the scheme exhibits higher efficiency and adaptability for power IoT systems. Srinivas *et al.* [19] introduced an anonymous signature-based authenticated key exchange mechanism for smart grids dependent on IoT. AVISPA verification and formal assessments validate its robustness for secure SM access in the smart grid. Despite this, the scheme suffers from partial key escrow problems and lacks man in the middle attack resistance.

Nyangaresi *et al.* [20] designed a novel SMs authentication algorithm for secure communication in smart grid networks. Rigorously analyzed for security, it ensures protection against various attacks while minimizing communication and computation overheads. Its robustness and efficiency make it suitable for resource-constrained smart grid devices. Liu *et al.* [21] introduced a new certificateless blind signature (CLBS) scheme with batch verification. They enhanced the power request system model within the smart grid to safeguard user privacy from potential eavesdropping threats. This proposed scheme simplifies certificate management and avoids hidden key escrow. It is validated for unforgeability using the random oracle model and is based on the ECDLP in terms of security. Notably, the scheme offers improved computational efficiency without requiring time-consuming bilinear pairing operations, making it advantageous compared to existing signature schemes in the smart grid domain. Chaudhry *et al.* [22] presented a novel authentication scheme for secure smart grid communication, ensuring direct device-to-device authentication. Tailored to combat key compromise impersonation and related threats, this scheme demonstrates heightened security and minimal communication costs compared to existing solutions. Leveraging EC and symmetric key operations, it establishes a secure channel within the smart grid infrastructure, verified for its resilience against known attacks. However, it suffers from impersonation attacks. Furthermore, their work yields bad performance due to dependence on EC, which results in high computational cost and communication overhead.

4. NETWORK MODEL

In this network model phase, the designed flow of our scheme is shown. As shown in Figure 1, the solar power stations act as primary energy sources, harnessing energy from sunlight and are equipped with monitoring systems to track energy output and some level of control mechanisms for operational management.

The control station serves as a central hub, receiving data from these stations through the grid, analyzing performance, and relaying optimization commands back to enhance energy production or address issues. The key generation center (KGC) plays a pivotal role; upon reception of a public parameter such as an entity identity, it generates partial private keys for the transmitting entity and sends them to that entity. As power service entities, SPs dynamically allocate the required power to individual users based on real-time messages received from the

deployed SMs in homes, smart cities, offices, and various locations. SPs leverage the data from SMs to orchestrate a responsive and personalized power allocation, optimizing energy distribution across diverse user environments. The proposed network model eliminates the reliance on digital certificates and employs partial private keys. The partial private keys, managed by the KGC, bolster communication security between the network actors. This innovative approach secures the transmission of energy data and enhances the overall resilience of the network, safeguarding against potential cyber threats or unauthorized access.

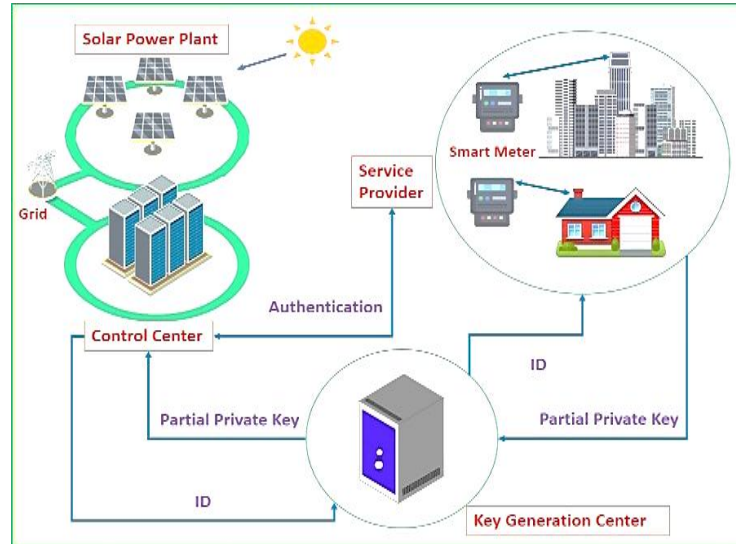


Figure 1. Flow of our proposed scheme

5. PROPOSED ELLIPTIC CURVE BASED CERTIFICATE-LESS AUTHENTICATION SCHEME

In this portion, the proposed method is described thoroughly through a table with different phases. Table 1 shows used symbols along with their precise explanation to depict the phases clearly.

Table 1. Symbols employed in the algorithm under consideration

Symbols	Explanation
KGC	Key generation center
h	Hash function
M_{pvt}, M_{pbk}	Master private key and master public key of KGC
$Pr_{pvt}key$	Partial private key
Y_{entity}	An entity (SP and CC) private key
X_{entity}	An entity (SP and CC) full public key
$FPvK_{entity}$	An entity (SP and CC) full private key
$rand$	Random number
R	Unique identifier
AV	Authentication vector

5.1. Initialization phase

This phase consists of three steps performed by the KGC to generate the necessary parameters:

- In the first step, KGC selects the cyclic group (G), which is generated by a point (P) on the (EC) over the finite field (Z_n), and its order is (q). Then, it selects a collision-resistant hash function (h).
- Then, the KGC selects a random secret value M_{pvt} with range $[1, q - 1]$ and uses it to compute its master public key $M_{pbk} = M_{pvt} \cdot P$. The secret value M_{pvt} is the KGC's master private key.
- When an entity (SP or control centre (CC)) sends its ID to the KGC, the KGC first computes $Q_{ID_{entity}} = h(ID_{entity})P$ and then uses it to compute the partial private keys of each entity $Pr_{pvt}key = M_{pvt} \cdot Q_{ID_{entity}}$. Afterwards, it transmits the respective partial private key to each entity.

5.2. Full key generation

In this phase, the CC and SP create a public key and a full private key using the following steps.

- Each entity selects a random number X_{entity} within the range $[1, q - 1]$ as its private key. Then, each entity generates its full private key, the combination of its chosen private key X_{entity} and partial private key $Pr_{pvt}key$ calculated by KGC.

$$FPvK_{entity} = X_{entity} \cdot Pr_{pvt}key$$

- Each entity generates its full public key as $Y_{entity} = FPvK_{entity} \cdot P$.

5.3. Authentication phase

After analysing the parameters of initial phase and full private key generation, in this phase, the phases of authentication mechanism have introduced. Here, CC first initiates a request to the SP, asking it to prove its legitimacy.

- In response, the SP performs the following steps.
 - Firstly, the SP generates a random number $rand$ and then uses it to compute $R = rand \cdot P$.
 - Then it computes authentication vector $AV = h(R || Y_{SP} || Y_{CC} || Timestamp)$ (1)
 - Then it computes a response $Resp = rand + (AV \cdot FPvK_{SP})$ (2)
 - The SP then sends the tuple $\{R, AV, Resp\}$ to CC.
- When the CC receives the tuple sent by SP, it performs the following steps to authenticate CC.
 - CC first compute $AV' = h(R || Y_{SP} || Y_{CC} || Timestamp)$.
 - CC then verifies if $Resp \cdot P = R + (AV' \cdot Y_{SP})$. (3)
 - If the above verification holds, CC will authenticate SP for further communication.

Upon successful authentication, CC and SP may establish a secure session using their shared secret for future communication.

5.4. Correctness proof

To ensure the correctness of authentication phase, we must need to accomplish the expected aligned values that are computed from both the CC and SP from the prior. The following proof demonstrate the steps of response verification that the equation holds using identical input parameters and thereby proving the correctness of the proposed authentication mechanism.

- When CC receives AV, it verifies if $AV' = h(R || Y_{SP} || Y_{CC} || Timestamp)$.
As SP compute the same equation $h(R || Y_{SP} || Y_{CC} || Timestamp)$ to get AV. The correction of this equation relies on a collision-resistant hash function because it behaves deterministically. In other words, for identical inputs, $h()$ will consistently yield the same output, and finding two distinct inputs that result in the same hash value is computationally impossible. Therefore, based on this assumption, $AV' = h(R || Y_{SP} || Y_{CC} || Timestamp)$.
- The CC verifies if $Resp \cdot P = R + (AV' \cdot Y_{SP})$.

$$a. R + (AV' \cdot Y_{SP}) = rand \cdot P + (AV' \cdot Y_{SP}) \quad (4)$$

$$\text{Since } Y_{SP} = FPvK_{SP} \cdot P$$

$$\text{Hence, } rand \cdot P + (AV' \cdot (FPvK_{SP} \cdot P)) = rand \cdot P + (AV' \cdot FPvK_{SP} \cdot P) = (rand + (AV' \cdot FPvK_{SP})) \cdot P$$

$$\text{As } AV' = AV$$

$$b. \text{ Hence, } (rand + (AV \cdot FPvK_{SP})) \cdot P \quad (5)$$

$$\text{Since } rand + (AV \cdot FPvK_{SP}) = Resp$$

$$c. Resp \cdot P \quad (\text{From (5)})$$

6. SECURITY ANALYSIS

This segment delves deeply into analyzing security attributes inherent in our work compared to existing methodologies. Extensive analysis of the current literature revealed several vulnerabilities, as detailed in Table 2.

Table 2. Security feature comparison

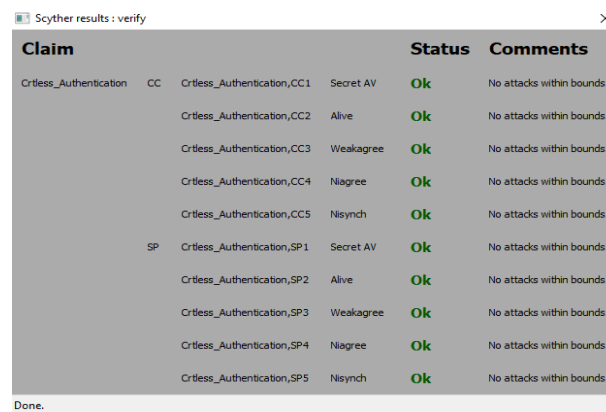
Security attributes	[16]	[19]	[22]	Proposed scheme
Authentication	✓	✓	✓	✓
Non repudiation	✓	✓	✓	✓
Integrity	✓	✓	✓	✓
Forward secrecy	×	✓	✓	✓
Anonymity	✓	×	✓	✓
Handle man in the middle attack	×	×	×	✓
Handle replay attack	×	✓	✓	✓
Handle Impersonation attack	✓	×	×	✓
Handle collision attack	✓	✓	✓	✓
Formal security validation	×	×	✓	✓

Note: ✓: yes; ×: no

Our proposed scheme stands out by significantly bolstering resilience against known attacks, as illustrated in Table 2. Particularly noteworthy is its adept mitigation of vulnerabilities present in prior work, including deficiencies in anonymity, forward secrecy, replay attack protection, impersonation attack protection, and protection against man-in-the-middle attacks. Through meticulous comparative analysis, our research highlights the enhanced security performance of the proposed approach in contrast to earlier work.

6.1. Security simulation

Scyther [23] is a formal verification tool for analyzing security protocols, notably those used in cryptographic systems. Automated analysis is a vital tool for discovering vulnerabilities and confirming the validity of security protocols. Scyther is programmed in Python and uses the extended Backus-Naur Form (eBNF) to design security protocols, making it flexible and expressive. The tool explores the state space of a given protocol using symbolic model-checking techniques, systematically examining various execution pathways [24]. Scyther builds a symbolic representation of the protocol during simulation, allowing for examining potential attacks or vulnerabilities in the system. Claims are helpful in the analysis process because they reflect security attributes or assertions. Scyther uses these assertions to determine whether a protocol meets specified security standards or whether vulnerabilities exist. Scyther's blend of formal approaches and automated analysis helps its effectiveness in discovering and correcting security flaws in cryptographic protocols [25]. We translated our protocol into the security protocol description language (SPDL) and leveraged Scyther to conduct a security assessment. The outcome, as illustrated in Figure 2, unequivocally demonstrates the safety and robustness of our protocol.



Claim	Status	Comments
Crtless_Authentication CC Crtless_Authentication,CC1 Secret AV	Ok	No attacks within bounds.
Crtless_Authentication,CC2 Alive	Ok	No attacks within bounds.
Crtless_Authentication,CC3 Weakagree	Ok	No attacks within bounds.
Crtless_Authentication,CC4 Niagree	Ok	No attacks within bounds.
Crtless_Authentication,CC5 Nisynch	Ok	No attacks within bounds.
SP Crtless_Authentication,SP1 Secret AV	Ok	No attacks within bounds.
Crtless_Authentication,SP2 Alive	Ok	No attacks within bounds.
Crtless_Authentication,SP3 Weakagree	Ok	No attacks within bounds.
Crtless_Authentication,SP4 Niagree	Ok	No attacks within bounds.
Crtless_Authentication,SP5 Nisynch	Ok	No attacks within bounds.

Done.

Figure 2. Security validation through scythe

7. PERFORMANCE ANALYSIS

Here, we thoroughly assess the performance of our methodology by comparing its computational cost and communication overhead with existing approaches.

7.1. Computational cost

The computational cost denotes the time needed to perform a particular algorithm or cryptographic operations. Lower computational cost indicates more efficient resource utilization, often desirable for practical applications, while higher computational cost may imply increase demand for hardware and potentially slower

performance. In the upcoming section, we contrast our proposed scheme with established literature [16], [19], and [22]. We focused on computationally intensive operations to achieve this objective, excluding those with negligible time impact. Specifically, we considered elliptic curve point multiplication (E_{cpm}), elliptic curve point addition (E_{cpa}), and hash function (h) operation. The findings inform our approach to experiments conducted in [26]. The experimental environment utilized in their study is - Intel (R) core (TM) i5-4210U CPU, RAM: 4 GB, clock speed: 2.4 GHz, operating system: Ubuntu 22.04.2 LTS, Python as programming language and PyCrypto for cryptographic library. Table 3 shows the time taken by various cryptographic operations. Additionally, Table 4 and Figure 3 comprehensively compare computational costs with existing work. The results unequivocally demonstrate that our approach surpasses the performance of existing methods in terms of computational cost.

Table 3. Time consumption by operations

Operation	Time taken by a single operation in milliseconds (ms)
$T_{E_{cpm}}$	1.029
$T_{E_{cpa}}$	0.016
T_h	0.043

Table 4. Computational cost in milliseconds

Scheme	No of operations	Time consumption in milliseconds (ms)
[16]	$10T_{E_{cpm}} + 6T_{E_{cpa}} + 6T_h$	10.644
[19]	$8T_{E_{cpm}} + 4T_{E_{cpa}} + 14T_h$	8.898
[22]	$8T_{E_{cpm}} + 2T_{E_{cpa}} + 8T_h$	8.608
Proposed scheme	$6T_{E_{cpm}} + 1T_{E_{cpa}} + 2T_h$	6.276

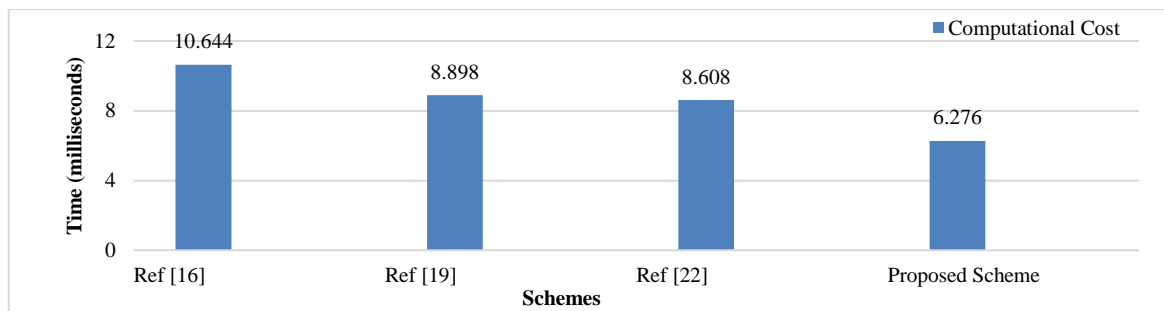


Figure 3. Computational cost comparison in terms of milliseconds

7.2. Communication overhead

The additional data (extra bits) accompanying the transmitted information is called communication overhead. This section describes the communication overhead comparison with the traditional existing work.

These extra bits are introduced to implement various security measures, ensuring the communication's confidentiality, integrity, and authenticity. Higher communication overhead is undesirable because it can lead to increased latency, reduced efficiency, and greater susceptibility to network congestion, compromising IoT systems' overall security and performance. The best practice in optimizing communication overhead is reducing the number of extra bits introduced while ensuring robust cyber security.

In this section, we compare our research with existing studies regarding communication overhead. Our analysis focuses on the bit size of the EC [E], set at 160 bits. The outcomes of this comparison are presented in Table 5 and Figure 4, showcasing the evident performance concerning communication overhead when juxtaposed with existing approaches.

Table 5. Communication overhead comparison with existing work

Scheme	Overall communication overhead	In bits
[16]	3[E]	480
[19]	4[E]	640
[22]	3[E]	480
Proposed scheme	2[E]	320

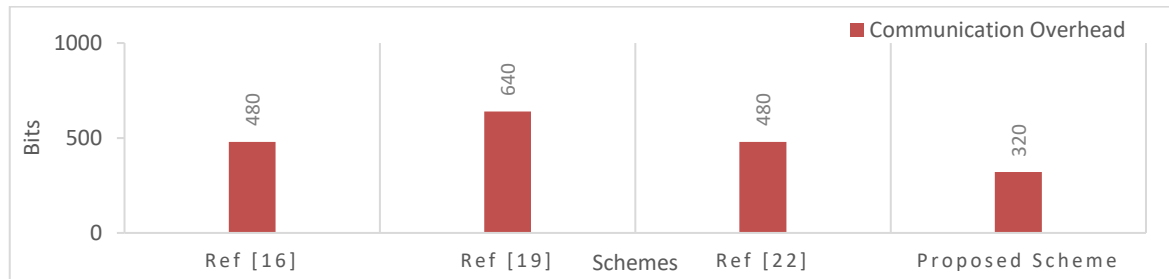


Figure 4. Communication overhead in bits

8. CONCLUSION

This article presents an innovative certificate-less authentication scheme for solar-based smart grids. ECC ensures adaptability to resource-constrained settings such as solar-based smart grids. Through comparative analysis with existing solutions, our approach demonstrates superior security attributes, including authentication, forward secrecy, anonymity, integrity, resilience to replay attacks, resilience to impersonation attacks, resilience to denial of service attacks, and resilience to man-in-the-middle attacks. The scheme's robustness is also substantiated by formal security validation using the Scyther tool. Furthermore, the work undergoes thorough performance evaluation, considering computational cost and communication overhead. In the future, we aim to integrate data aggregation for privacy preservation and incorporate hyper ECC to enhance performance, making it even more effective for resource-constrained environments.

ACKNOWLEDGMENTS

The authors like to express their sincere gratitude to Faculty of Engineering and Technology, University of Scholars, Dhaka, Bangladesh, for providing enormous support and cooperation for successful completion of this research endeavour and providing the research facilities.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Reduanul Bari Shovon	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ashif Mohammad	✓	✓		✓	✓	✓	✓		✓		✓	✓	✓	
Rimi Das				✓	✓		✓	✓		✓	✓		✓	✓
Tuhin Hossain			✓			✓	✓		✓	✓	✓	✓		✓
Md Ahasun Habib		✓				✓				✓				✓
Ratul														
Ronjon Kundu					✓		✓	✓		✓	✓			✓
Md. Ahsan Arif			✓	✓	✓			✓		✓		✓	✓	✓

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

INFORMED CONSENT

We have obtained informed consent from all individuals included in this study.

DATA AVAILABILITY




Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES




- [1] O. M. Butt, M. Zulqarnain, and T. M. Butt, "Recent advancement in smart grid technology: future prospects in the electrical power network," *Ain Shams Engineering Journal*, vol. 12, no. 1, pp. 687–695, Mar. 2021, doi: 10.1016/j.asej.2020.05.004.
- [2] S. A. Aleem, S. M. S. Hussain, and T. S. Ustun, "A review of strategies to increase pv penetration level in smart grids," *Energies*, vol. 13, no. 3, pp. 1–28, Feb. 2020, doi: 10.3390/en13030636.
- [3] C. Lamnatou, D. Chemisana, and C. Cristofari, "Smart grids and smart technologies in relation to photovoltaics, storage systems, buildings and the environment," *Renewable Energy*, vol. 185, pp. 1376–1391, Feb. 2022, doi: 10.1016/j.renene.2021.11.019.
- [4] N. M. Kumar *et al.*, "Distributed energy resources and the application of AI, IoT, and blockchain in smart grids," *Energies*, vol. 13, no. 21, pp. 1–42, Nov. 2020, doi: 10.3390/en13215739.
- [5] D. Faquir, N. Choularas, V. Sofia, K. Olga, and L. Maglaras, "Cybersecurity in smart grids, challenges and solutions," *AIMS Electronics and Electrical Engineering*, vol. 5, no. 1, pp. 24–37, 2021.
- [6] A. Shamir, "Identity-based cryptosystems and signature schemes," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 196 LNCS, pp. 47–53, 1985, doi: 10.1007/3-540-39568-7_5.
- [7] C. Gentry, "Certificate-based encryption and the certificate revocation problem," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2656, 2003, pp. 272–293, doi: 10.1007/3-540-39200-9_17.
- [8] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2894, pp. 452–473, 2003, doi: 10.1007/978-3-540-40061-5_29.
- [9] S. Majumder, S. Ray, D. Sadhukhan, M. K. Khan, and M. Dasgupta, "ECC-coap: elliptic curve cryptography based constraint application protocol for internet of things," *Wireless Personal Communications*, vol. 116, no. 3, pp. 1867–1896, Feb. 2021, doi: 10.1007/s11277-020-07769-2.
- [10] N. Kobitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987, doi: 10.1090/S0025-5718-1987-0866109-5.
- [11] P. Zhou, C. Jin, Z. Chen, G. Chen, and L. Wang, "An efficient heterogeneous signcryption scheme for internet of things," *Pervasive and Mobile Computing*, vol. 94, Aug. 2023, doi: 10.1016/j.pmcj.2023.101821.
- [12] G. S. Rao, G. Thumbar, R. B. Amarapu, G. N. Bhagya, and P. V. Reddy, "A new lightweight and secure certificateless aggregate signcryption scheme for industrial internet of things," *IEEE Internet of Things Journal*, vol. 11, no. 6, pp. 10563–10574, Mar. 2024, doi: 10.1109/JIOT.2023.3327503.
- [13] T. F. Vallent, D. Hanyurwimfura, H. Kim, and C. Mikeka, "Certificate-less authenticated key agreement scheme with anonymity for smart grid communications," *Journal of Intelligent & Fuzzy Systems*, vol. 43, no. 2, pp. 1859–1869, Jun. 2022, doi: 10.3233/JIFS-219287.
- [14] A. Badshah *et al.*, "LAKE-bsg: lightweight authenticated key exchange scheme for blockchain-enabled smart grids," *Sustainable Energy Technologies and Assessments*, vol. 52, Aug. 2022, doi: 10.1016/j.seta.2022.102248.
- [15] S. Shukla, S. Thakur, and J. G. Breslin, "Secure communication in smart meters using elliptic curve cryptography and digital signature algorithm," in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, IEEE, Jul. 2021, pp. 261–266, doi: 10.1109/CSR51186.2021.9527947.
- [16] L. Deng and R. Gao, "Certificateless two-party authenticated key agreement scheme for smart grid," *Information Sciences*, vol. 543, pp. 143–156, Jan. 2021, doi: 10.1016/j.ins.2020.07.025.
- [17] A. A. Khan, V. Kumar, M. Ahmad, and S. Rana, "LAKAF: lightweight authentication and key agreement framework for smart grid network," *Journal of Systems Architecture*, vol. 116, pp. 1–11, Jun. 2021, doi: 10.1016/j.sysarc.2021.102053.
- [18] W. Cui, R. Cheng, K. Wu, Y. Su, and Y. Lei, "A certificateless authenticated key agreement scheme for the power iot," *Energies*, vol. 14, no. 19, pp. 1–13, Oct. 2021, doi: 10.3390/en14196317.
- [19] J. Srinivas, A. K. Das, X. Li, M. K. Khan, and M. Jo, "Designing anonymous signature-based authenticated key exchange scheme for internet of things-enabled smart grid systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 7, pp. 4425–4436, Jul. 2021, doi: 10.1109/TII.2020.3011849.
- [20] V. O. Nyangaresi, M. Abd-Elnaby, M. M. A. Eid, and A. N. Z. Rashed, "Trusted authority based session key agreement and authentication algorithm for smart grid networks," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 9, Sep. 2022, doi: 10.1002/ett.4528.
- [21] S. Liu, Y. Zhu, and R. Wang, "Pairing-free certificateless blind signature scheme for smart grid," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 10145–10156, Nov. 2022, doi: 10.1016/j.jksuci.2022.10.012.
- [22] S. A. Chaudhry, J. Nebhan, K. Yahya, and F. Al-Turjman, "A privacy enhanced authentication scheme for securing smart grid infrastructure," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 7, pp. 5000–5006, Jul. 2022, doi: 10.1109/TII.2021.3119685.
- [23] C. J. F. Cremers, "Scyther: semantics and verification of security protocols," Ph.D. Dissertation, Eindhoven University of Technology, 2006, doi: 10.6100/IR614943.
- [24] C. J. F. Cremers, "The scyther tool: verification, falsification, and analysis of security protocols," in *Computer Aided Verification*, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 414–418, doi: 10.1007/978-3-540-70545-1_38.
- [25] N. El Madhoun, E. Bertin, M. Badra, and G. Pujolle, "Towards more secure EMV purchase transactions," *Annals of Telecommunications*, vol. 76, no. 3–4, pp. 203–222, Apr. 2021, doi: 10.1007/s12243-020-00784-1.
- [26] V. O. Nyangaresi *et al.*, "A symmetric key and elliptic curve cryptography-based protocol for message encryption in unmanned aerial vehicles," *Electronics*, vol. 12, no. 17, pp. 1–20, Aug. 2023, doi: 10.3390/electronics12173688.

BIOGRAPHIES OF AUTHORS






Reduanul Bari Shovon    received a bachelor of engineering in computer science and engineering from North South University, Dhaka in 2018. He received a master of engineering also in computer science and engineering from Jahangirnagar University, Dhaka, in 2020. He has been a full-time Lecturer at the Department of Computer Science and Engineering in University of Scholars, Banani, Dhaka since 2021 and currently is a Senior Lecturer at the same institution. He has more than five years of experience in teaching with a specialization in artificial intelligence, renewable energy, deep learning, and natural language processing. He can be contacted at email: reduanul.bari@ius.edu.bd.






Ashif Mohammad    received a bachelor of engineering in electrical and electronic engineering from Ahsanullah University of Science and Technology and M.S. in renewable energy technology from the University of Dhaka. He is currently working as a Private Secretary to the Information Commissioner in Information Commission Bangladesh. He has more than eight years of engineering experience, specialising in renewable energy, artificial intelligence, and cybersecurity. He can be contacted at email: ashif028628@gmail.com.






Rimi Das    is pursuing her master's in electrical and computer engineering at Idaho State University and has completed another master's in renewable energy technology from the University of Dhaka. She has 10 years of experience in various industries, including power generation, and solar energy. She is currently researching microwave and RF antenna design and has also conducted multiple research papers on renewable energy. She can be contacted at email: rimidas@isu.edu.






Tuhin Hossain    received a bachelor of engineering in computer science and engineering from Daffodil International University and M.Sc. in computer science and engineering from Jahangirnagar University, Savar, Dhaka. Currently, he is pursuing as a Lecturer in the Department of Computer Science and Engineering at the University of Scholars, Banani, Dhaka. His current research area focuses on machine learning, deep learning, computer vision, natural language processing, and network automation. He can be contacted at email: tuhin@ius.edu.bd.






Md Ahasun Habib Ratul    is an experienced teacher with a robust background in the British Council and International Baccalaureate (IB) curriculum for Advanced Computer Science and ICT, and dedicated his career to fostering critical thinking and global awareness in students. His interest area of cybersecurity and machine learning for his thesis exploring innovative approaches using machine learning techniques to enhance cybersecurity. He can be contacted at email: md.ahasun.habib.ratul@gmail.com.



Ronjon Kundu    is a graduate of The University of Western Australia (UWA), specializing in Data Science. He holds an M.S. degree from UWA. His current research focuses on machine learning, deep learning, natural language processing, and AI, contributing to advancements in data science. He can be contacted at email: babukundu@gmail.com.



Md. Ahsan Arif    received his graduation and post-graduation in computer science and engineering from University of Madras, India. He is currently working as an Associate Professor and Head of the Department in Computer Science and Engineering, University of Scholars, Banani, Dhaka. He can be contacted at email: ahsan@ius.edu.bd.